Vulnerability Assessment Report: Metasploitable

1. Introduzione

Questo report documenta i risultati di una scansione di vulnerabilità effettuata sulla macchina Metasploitable utilizzando Nessus. L'obiettivo è identificare e mitigare le vulnerabilità presenti.

2. Metodologia

La scansione è stata configurata come segue:

- Tipo di scansione: Basic Network Scan

- Target: Indirizzo IP della macchina Metasploitable

- Porte scansionate: 21, 22, 80, 139, 445, 3306

3. Risultati della Scansione

| Porta | Servizio | Vulnerabilità | Gravità |

|-------|----------|----------------|---------|

| 21 | FTP | Accesso anonimo consentito | Alta |

| 22 | SSH | Attacchi brute-force possibili | Media |

| 80 | HTTP | Versione obsoleta di Apache | Critica |

4. Dettagli delle Vulnerabilità

Porta: 21 (FTP)

- **Descrizione**: Il servizio FTP consente accessi anonimi.

- **Gravità**: Alta

- **Impatto**: Gli attaccanti possono accedere al sistema senza autenticazione.

- **Soluzione**: Disabilitare gli accessi anonimi nel file di configurazione del server FTP.

Porta: 22 (SSH)

- **Descrizione**: Il servizio SSH è vulnerabile ad attacchi brute-force.

- **Gravità**: Media

- **Impatto**: Gli attaccanti possono ottenere l'accesso non autorizzato tramite tentativi di login ripetuti.

- **Soluzione**: Implementare l'uso di chiavi SSH, limitare gli accessi tramite firewall, e configurare il file `sshd_config` per limitare i tentativi di accesso.

Porta: 80 (HTTP)

- **Descrizione**: Il servizio HTTP utilizza una versione obsoleta di Apache con vulnerabilità note.

- **Gravità**: Critica

- **Impatto**: Gli attaccanti possono sfruttare vulnerabilità note per compromettere il server.

- **Soluzione**: Aggiornare Apache alla versione più recente e seguire le linee guida di sicurezza per la configurazione.

5. Raccomandazioni di Remediation

1. Disabilitare gli accessi anonimi per il servizio FTP.

2. Implementare misure di sicurezza avanzate per il servizio SSH.

3. Aggiornare il server Apache alla versione più recente e configurarlo seguendo le best practices.

6. Conclusioni

La scansione ha rilevato diverse vulnerabilità critiche e alte che richiedono immediata attenzione. Si raccomanda di implementare le soluzioni proposte per mitigare i rischi associati.

Vulnerability Assessment Executive Summary: Metasploitable

1. Introduzione

Questo report fornisce una sintesi delle vulnerabilità identificate sulla macchina Metasploitable. L'obiettivo è ottenere l'approvazione per implementare le misure di sicurezza necessarie.

2. Sintesi dei Risultati

Porta	Servizio	Vulnerabilità	Gravità
21	FTP	Accesso anonimo consentito	Alta
22	SSH	Attacchi brute-force possibili	Media
80	HTTP	Versione obsoleta di Apache	Critica

3. Impatto delle Vulnerabilità

4. Raccomandazioni

- Disabilitare gli accessi anonimi per il servizio FTP.

- Migliorare la sicurezza del servizio SSH implementando l'uso di chiavi SSH e limitando gli accessi tramite firewall.

- Aggiornare il server Apache alla versione più recente.

5. Conclusioni

Le vulnerabilità identificate presentano rischi significativi per la sicurezza della nostra infrastruttura. Si raccomanda di implementare le misure correttive proposte per mitigare questi rischi e proteggere i nostri asset critici.